Colliding Message Pairs for 23 and 24-step SHA-512

Somitra Kumar Sanadhya* and Palash Sarkar

Applied Statistics Unit,
Indian Statistical Institute,
203, B.T. Road, Kolkata,
India 700108.
somitra_r@isical.ac.in, palash@isical.ac.in

1st September, 2008

Abstract. Recently, Indesteege et al. [1] had described attacks against 23 and 24-step SHA-512 at SAC '08. Their attacks are based on the differential path by Nikolić and Biryukov [2]. The reported complexities are $2^{44.9}$ and 2^{53} calls to the respective step reduced SHA-512 hash function. They provided colliding message pairs for 23-step SHA-512 but did not provide a colliding message pair for 24-step SHA-512. In this note we provide a colliding message pair for 23-step SHA-512 and the first colliding message pair for 24-step SHA-512. Our attacks use the differential path first described by Sanadhya and Sarkar at ACISP '08 [3]. The complexities of our attacks are $2^{16.5}$ and $2^{34.5}$ calls to the respective step reduced SHA-512 hash function. Complete details of the attacks will be provided in an extended version of this note.

1 Colliding Message Pairs

In [4], 23 and 24-step SHA-256 attacks are described. Similar attacks will also work for 23 and 24-step SHA-512. Complete details of these attacks will be provided later. For notation see [4].

A set of suitable values of δ_2, α, λ, μ and γ for the 23-step SHA-512 collision is the following. $\delta_2 =$ `0x600000000237`, $\alpha =$ `0x7201b90f9f8df85e`, $\lambda =$ `0x3e000007ffdc9`, $\mu =$ `0x43fffff800001` and $\gamma =$ `0x1`.

Values of the constants for 24-step SHA-512 collision is the following. $\delta_1 =$ `0x200000000008`, $\delta_2 =$ `0x600000000237`, $\alpha =$ `0x7201b90f9f8df85e`, $\lambda =$ `0x3e000007ffdc9`, $\mu =$ `0x45fffff800009`, $\gamma =$ `0x1`. The colliding message pairs are provided in Table 1 and Table 2 next.

* This author is supported by the Ministry of Information Technology, Govt. of India.

Table 1. Colliding message pair for 23-step SHA-512 with standard IV.

W_1	0-3	b9fa6fc4729ca55c	8718310e1b3590e1	1d3d530cb075b721	99166b30ecbdd705
	4-7	27ed55b66c090b62	754b2163ff6feec5	6685f40fd8ab08f8	590c1c0522f6fdfd
	8-11	b947bb4013b688c1	d9d72ca8ab1cac04	69d0e120220d4edc	30a2e93aeef24e3f
	12-15	84e76299718478b9	f11ae711647763e5	d621d2687946e862	0ee57069123ecc8b
W_2	0-3	b9fa6fc4729ca55c	8718310e1b3590e1	1d3d530cb075b721	99166b30ecbdd705
	4-7	27ed55b66c090b62	754b2163ff6feec5	6685f40fd8ab08f8	590c1c0522f6fdfd
	8-11	b947bb4013b688c2	d9d72ca8ab1cac03	69d0e120220d4edc	30a3493aeef25076
	12-15	84e76299718478b9	f11ae711647763e5	d621d2687946e862	0ee57069123ecc8b

Table 2. Colliding message pair for 24-step SHA-512 with standard IV.

W_1	0-3	dedb689cfc766965	c7b8e064ff720f7c	c136883560348c9c	3747df7d0cf47678
	4-7	855e17555cfedc5f	88566babccaa63e9	5dda9777938b73cd	b17b00574a4e4216
	8-11	86f3ff48fd12ea19	cd15c6f8d6da38ce	5e2c6b7b0411e70b	36ed67e93a794e66
	12-15	1b65e96b02767821	04d0950089db6c68	5bc9b9673e38eff3	b05d879ad024d3fa
W_2	0-3	dedb689cfc766965	c7b8e064ff720f7c	c136883560348c9c	3747df7d0cf47678
	4-7	855e17555cfedc5f	88566babccaa63e9	5dda9777938b73cd	b17b00574a4e4216
	8-11	86f3ff48fd12ea19	cd15c6f8d6da38ce	5e2c6b7b0411e70c	36ed67e93a794e65
	12-15	1b66096b02767829	04d0f50089db6e9f	5bc9b9673e38eff3	b05d879ad024d3fa

References

1. Sebastiaan Indesteege, Florian Mendel, Bart Preneel, and Christian Rechberger. Collisions and other Non-Random Properties for Step-Reduced SHA-256. To appear in *SAC 2008*. Available at `http://eprint.iacr.org/2008/131`.
2. Ivica Nikolić and Alex Biryukov. Collisions for Step-Reduced SHA-256. In Kaisa Nyberg, editor, *Fast Software Encryption, 15th International Workshop, FSE 2008, Lausanne, Switzerland, March 26-28, 2008*, volume Pre-proceedings version of *Lecture Notes in Computer Science*, pages 1–16. Springer, 2008.
3. Somitra Kumar Sanadhya and Palash Sarkar. Non-Linear Reduced Round Attacks Against SHA-2 Hash family. In Yi Mu and Willy Susilo, editors, *Information Security and Privacy - ACISP 2008, The 13th Australasian Conference, Wollongong, Australia, 7-9 July 2008, Proceedings*, volume 5107 of *Lecture Notes in Computer Science*. Springer, 2008.
4. Somitra Kumar Sanadhya and Palash Sarkar. Attacking Step Reduced SHA-2 Family in a Unified Framework. *Cryptology eprint Archive*, June 2008. Available at `http://eprint.iacr.org/2008`.